
SUPPLEMENT NO. 6 --TECHNICAL QUESTIONNAIRE FOR ENCRYPTION ITEMS

(a) For all encryption items:

(1) State the name(s) of each product being submitted for classification or other consideration (as a result of a request by BIS) and provide a brief non technical description of the type of product (e.g., routers, disk drives, cell phones, and chips) being submitted, and provide brochures, data sheets, technical specifications or other information that describe the item(s).

(2) Indicate whether there have been any prior classifications or registrations of the product(s), if they are applicable to the current submission. For products with minor changes in encryption functionality, you must include a cover sheet with complete reference to the previous review (Commodity Classification Automated Tracking System (CCATS) number, Encryption Registration Number (ERN), Export Control Classification Number (ECCN), authorization paragraph) along with a clear description of the changes.

(3) Describe how encryption is used in the product and the categories of encrypted data (e.g., stored data, communications, management data, and internal data).

(4) For ‘mass market’ encryption products, describe specifically to whom and how the product is being marketed and state how this method of marketing and other relevant information (e.g., cost of product and volume of sales) are described by the Cryptography Note (Note 3 to Category 5, Part 2).

(5) Is any “encryption source code” being provided (shipped or bundled) as part of this offering? If yes, is this source code publicly available source code, unchanged from the code obtained from an open source web site, or is it proprietary “encryption source code?”

(b) For classification requests and other submissions for an encryption commodity or software, provide the following information:

(1) Description of all the symmetric and asymmetric encryption algorithms and key lengths and how the algorithms are used, including relevant parameters, inputs and settings. Specify which encryption modes are supported (e.g., cipher feedback mode or cipher block chaining mode).

(2) State the key management algorithms, including modulus sizes that are supported.

(3) For products with proprietary algorithms, include a textual description and the source code of the algorithm.

(4) Describe the pre-processing methods (e.g., data compression or data interleaving) that are applied to the plaintext data prior to encryption.

(5) Describe the post-processing methods (e.g., packetization, encapsulation) that are applied to the cipher text data after encryption.

(6) State all communication protocols (e.g., X.25, Telnet, TCP, IEEE 802.11, IEEE 802.16, SIP ...) and cryptographic protocols and methods (e.g., SSL, TLS, SSH, IPSEC, IKE, SRTP, ECC, MD5, SHA, X.509, PKCS standards...) that are supported and describe how they are used.

(7) Describe the encryption-related Application Programming Interfaces (APIs) that are implemented and/or supported. Explain which interfaces are for internal (private) and/or external (public) use.

(8) Describe the cryptographic functionality that is provided by third-party hardware or software encryption components (if any). Identify the

manufacturers of the hardware or software components, including specific part numbers and version information as needed to describe the product. Describe whether the encryption software components (if any) are statically or dynamically linked.

(9) For commodities or software using Java byte code, describe the techniques (including obfuscation, private access modifiers or final classes) that are used to protect against decompilation and misuse.

(10) State how the product is written to preclude user modification of the encryption algorithms, key management and key space.

(11) Describe whether the product meets any of the §740.17(b)(2) criteria. Provide specific data for each of the parameters listed, as applicable (e.g., maximum aggregate encrypted user data throughput, maximum number of concurrent encrypted channels, and operating range for wireless products).

(12) For products which incorporate an “open cryptographic interface” as defined in part 772 of the EAR, describe the cryptographic interface.

(c) For classification requests for hardware or software “encryption components” other than source code (i.e., chips, toolkits, executable or linkable modules intended for use in or production of another encryption item) provide the following additional information:

(1) Reference the application for which the components are used in, if known;

(2) State if there is a general programming interface to the component;

(3) State whether the component is constrained by function; *and*

(4) Identify the encryption component and include the name of the manufacturer, component model number or other identifier.

(d) For classification requests for “encryption source code” provide the following information:

(1) If applicable, reference the executable (object code) product that was previously classified by BIS or included in an encryption registration to BIS;

(2) Include whether the source code has been modified, and the technical details on how the source code was modified; *and*

(3) *Upon request*, include a copy of the sections of the source code that contain the encryption algorithm, key management routines and their related calls.